Systems Support Services - Code 5595

Desktop

Latest Information from the NRL Labwide ADP Program and the NRL Systems Support Team

http://amp.nrl.navy.mil/code5595 March 27, 2001

Secure Shell Software
SSH Tools Available from CCS

The Center for Computational Sciences (CCS) has several free Secure Shell (SSH) tools for encrypted communication of passwords and information between computers. There are two major versions of the Secure Shell protocol, SSH1 and SSH2. SSH2 protocol is a rewrite of SSH1 protocol with improvements to security.

For the ssh2 protocol, **OpenSSH** 2.5.1 is available. It provides support for SSH1 and SSH2 protocols. The operating systems it supports include: OpenBSD, NetBSD, FreeBSD, AIX, HP/UX, IRIX, Linux, NeXT, SCO, SNI/Reliant Unix, Solaris, Digital Unix/Tru64/OSF and MacOS X.

OpenSSH 2.5.1 includes server and client programs as well as secure copy, secure FTP and secure tunneling capabilities. For secure telnet from windows computers to ssh2 server, use:

- **PuTTy**

For secure telnet from Mac computers to ssh2 server, use:

- **MacSSH**

For the older **SSH 1** protocol, the ssh-1.2.27.tar.gz package is available for all *mainstream* unix machines. This package *must be patched* with the ssh-1.2.31-deattack.patch which addresses recent SSH-1 vulnerabilities. The ssh-1.2.31 patch can be applied to the ssh-1.2.27.tar.gz package which includes server and client programs as well as secure copy and secure tunneling. Since the SSH1 protocol seems more vulnerable to attacks, it is highly advisable to check your wrappers to make sure that you are only allowing your own subnet access to your equipment.

For secure telnet from windows computers to an ssh1 unix server, use:

- **PuTTy**
- **QVT/Net** with ssh1,or
- **Teraterm Pro with TTSSH** .

For a secure ftp from windows computers to an ssh1 unix server, use:

- **Secure iXplorer**

For secure telnet from a Mac computers to ssh1 unix server, use:

- **Nifty Telnet**

All the above mentioned programs can be downloaded from:

http://amp.nrl.navy.mil/code5595/

In the lower left-hand frame, click on the link, *Site/Volume Discount Licenses* and then select the software you want to download.

For help on the implementation of SSH or wrappers, send email to *syssupport@nrl.navy.mil*. ❑

NRL Dial-in
Password Changes

Password aging has been added to local and toll-free accounts. Users will be prompted to change passwords as of 3/13/2001, and then on an annual basis. In order to make the password change, you must follow the instructions provided below on how to bring up a terminal window. If you enter your username and password every time you dial in, here's what to expect.

For local dial-in accounts: dial 202-404-3036 or 202-767-1101 . **For 1-800 dial-in accounts**: dial 1-800-648-6839. NOTE: NRL sessions from 202-404-xxxx and 202-767-xxxx can be used to test accounts **before** going on travel.

```
login: username
Password: current_password
Password expired.
Enter new password:
Response: new_password
New password accepted
PPP session from ...
```

(click on "Done" or press key "F7" to continue)

continued on page 4

Desktop

Naval Research Laboratory
4555 Overlook Ave., S.W.
Washington, DC 20375-5320

Editor, Code 5595.2
Phone: (202) 767-5853
via e-mail: syssupport@nrl.navy.mil
published periodically
distributed to: distribution list d at NRL-DC

◆

Upcoming Instructor-led Courses

To register for these courses, please visit the Code 5595 Training web page at **amp.nrl.navy.mil/code5595;** course descriptions are also available there. If there are any questions concerning the courses please contact *Ralph Thompson* on (202) 404-3143, or **thompsor@ccs.nrl.navy.mil**.

All courses will be held in the Building 72 Annex. Classes start at 9:00 a.m. The courses are presented by a Microsoft Certified Instructor. Class size is limited to 12 students per course.

1.Implementing & Supporting TCP/IP on Windows NT (5 days)

*Dates:*May 8 - 10 & May 15, 16

*Overview:*Students will learn the skills required to install, configure, use and support TCP/IP on Windows NT Server 4.0.

*Prerequisites:*Windows NT System Architecture and Network Support, or equivalent knowledge.

2. Internet Information Server; Web Site Administration (3 days)

*Dates:*June 19 - 21

*Overview:*Students will learn how to install, configure, and manage a web site based on Microsoft's IIS 4.0

*Prerequisites:*Windows NT System Architecture and Network Support,or equivalent knowledge and Implementing & Supporting TCP/IP. ❑

CBT Frequently Asked Questions

Q1. What student number do I enter?

• If you have previously self-registered, enter the same number you self-registered with, or

• Enter "self" and follow the process for self registration.

Students cannot access courses unless they have a valid student number. Students may self-register for classes, creating their own student number. We suggest using your phone number so that you will easily remember your number and so that Human Resources or the web master for this site may contact you regarding your class if necessary.

Q2. Why are there only CBT Player downloads for Windows clients?

Currently there are only CBT players for windows clients. In the next month or two, a new web-based player will be available which will give other clients (Macintosh, Unix) access to the courses. We apologize for the delay in accessibility for these clients and are working to acquire and configure the new player as soon as it becomes available.

If you use a system other than a windows-based system and are anxious to view these courses, Code 5595 is offering access to a Citrix Metraframe server. This server will allow Unix and Macintosh systems to access windows-based applications. For more information, please contact Diane Martin on 404-4195.

Please check back periodically for updates to courseware and players.

For a complete course listing, please access web page:

amp.nrl.navy.mil/code5595/ ccs-training

Q3. Will I get credit in my Official Personnel Folder (OPF) for taking on-line courses?

In the near future, a monthly update to the Defense Civilian Personnel Data System (DCPDS) is planned. It will be up to you to decide whether or not you want your on-line classes to be listed on your OPF. PLEASE NOTE: Your official record will only store the most recent 35 classes. As you take classes, older classes will fall off of the list available from DCPDS.

As an alternative, you will be able to obtain a list of your completed courses from this web site. That option will be available soon, please check back periodically for updates.

Q4. Will other courses be added to the current list of courses?

We are currently researching other computer based training titles. If you know of other course selections or areas of interest, please utilize our feedback link to provide this information. We will look into your suggested courses and will add them to the courseware listing if there is sufficient interest and the courseware is compatible with our web site.

In addition, we have several video-based training titles that are also available for check-out. These selections will be available for check-out on-line very shortly.

Q5. Question not answered ?

Please send E-Mail to **syssupport@nrl.navy.mil** or call *Diane Martin* on 202-404-4195. ❑

Configuring TCP Wrappers at NRL

Most NRL UNIX-based systems use the TCP Wrappers software package to restrict their in-bound, network-related services such as telnet, ftp, etc. to a set of client systems as appropriate. Two configuration files, **/etc/hosts.allow** and **/etc/hosts.deny**, specify the access control.

At NRL, the customary practice is to be exclusive, i.e. completely restrict access in hosts.deny; then selectively allow client access in hosts.allow for:

- specific hosts,
- subnets,
- or all NRL systems.

The basic format of a host.deny or host.allow is the same. Each line contains <*service* `:` *client*>. A typical hosts.deny contains one line:

```
ALL:ALL
```

This denies all wrapped services to all hosts on the net.

The hosts.allow file is more interesting. Some examples may be instructive. To allow ftp access from any NRL system (i.e.: about 3000 users), the system administator would enter the client specification as a set of network masks:

```
in.ftpd:\
132.250.0.0/255.255.0.0,\
134.207.0.0/255.255.0.0,\
128.60.0.0/255.255.0.0,\
127.0.0.0/255.255.255.0
```

Note that your ftp service may be named **ftpd**, check your entry in /etc/inetd.conf.

Also note that this is one line, the <RETURN>s are escaped.

Suppose that your system is on the 112 subnet, and you wanted to **restrict telnet access to hosts on that subnet**:

```
in.telnetd:\
132.250.112.0/255.255.255.0
```

The usual problem with this restriction is that the staff still needs to access the system from home via dialin. The **network access for the NRL dialin accounts** can be covered by allowing:

```
132.250.200.0/255.255.248.0
```

For NRL VPN accounts use:

```
132.250.216.0/255.255.255.0
```

Of course, access can be even more restrictive - you can specify individual hosts. For instance, to allow telnet exclusively from host curie:

```
in.telnetd:\
curie.nrl.navy.mil
```

Of course, you can use any combination of these in hosts.allow. If your system doesn't have TCP Wrappers installed, you will find install instructions at:

http://security.nrl.navy.mil
/isso/tcpwrappers

If you have any questions or need assistance with TCP Wrappers intallation or configuration, please send email to *syssupport@nrl.navy.mil*. ❑

Visit our recently revised web pages!

http:/amp.nrl.navy.mil/code5595

Restricting Root Logins to the Console

On UNIX / Linux systems, as a general rule, it is considered good security practice to restrict root logins to the console. This means that anyone accessing the root account via the network will have to login to a regular user account and then use the "/bin/su" command to become root.

In case of a break-in, the advantage to this setup is that your system logs will show which user account was compromised in order to run the su command and gain root privileges. If remote root logins were allowed, the hacker would not have to reveal a compromised user account.

The method for restricting root logins to the console, varies from system to system. Please find below some pointers for several popular versions of UNIX.

```
Solaris & IRIX:
     /etc/default/login
     CONSOLE = /dev/console

AIX: /etc/security/user
     root:#stanza
     rlogin = false

HPUX:/etc/securetty
     console

LINUX:/etc/securetty
     # remove pseudo terms;
     ttyp1, ttyp2, etc.
```

As always, you should change the root password everytime someone who knows the password leaves your site or whenever you think security has been compromised. NRL's password policy is available at:

http://security.nrl.navy.mil
/nrl/compusec.htm

If you have any questions about root logins, please send email to *syssupport@nrl.navy.mil*. ❑

NRL Dial-in
Password Changes

continued from page 1

If you use an automated dialin script, you will need to select an interactive login method (such as Pop-up terminal for Windows or Hyper terminal for Macs) to make the password change. Automated dialin scripts may not recognize the "*Password expired*" prompt, and repeated failed attempts will result in your account being blacklisted (you will then need to contact us to unblock the account).

An alternative procedure to initiate the password change at anytime is as follows:

- Type in your username at the **login** prompt.
- Type in "passwd" at the **password** prompt, without the quotes.
- Enter your password at the **current password response** prompt.
- Now enter your new password at the **new password response** prompt.

Example

```
login: mishra
Password: passwd
Current password:
Response: i8j6d9ml
New password:
Response: uB05mEjc
```

NOTE: If the password change was successful, an PPP session will start immediately. At this point, you will have the option of continuing with the PPP session or disconnecting to log out.

Please visit our web page at **http://netgroup.nrl.navy.mil/dial-in/dial-in.html** or contact us at *dialin@nrl.navy.mil* or 767-3903 for further assistance. ❑

Dialin Window-opening Instructions

• Windows 2000

a) Go to *start->program->accessories->communications-> network and dial up connections.*
b) Right click on the properties of the dial-in connection you have, either *local* or *800*.
c) Click on the *security* tab.
d) Check the *show terminal window.*
e) This will bring up a terminal window after dialing in.

• Windows 98

a) Go to *start->programs->accessories->communications-> dial up networking*.
b) Click on the profile you have, either *local* or *800*.
c) Now right click on that profile and select *properties*.
d) Click on the *configure modem* button.
e) Now select the *options* tab at the top of the new window.
f) Check the box *Bring up terminal window after dialing*.
g) This will bring up a terminal window after dialing in.

• Windows NT

a) Go to *start->program->accessories->dial up networking*.
b) Select the phonebook entry to dial, either *local* or *NRL 800*.
c) Click on the button *more*.
d) Select *edit entry and modem properties.*
e) Click on the tab *Script*.
f) Check the *Pop up a terminal Window Entry.*
g) This will bring up a terminal window after dialing

• MacOS

a) Click on Mac's *Apple* .
b) **MacOS 8.x.x**
Select *Control Panel*, then *PPP.*
A PPP dialog box will appear .
MacOS 9.xx
Select *Control Panel*, then *Remote Access*.
A Remote Access dialog box will appear.
c) Select the tab *protocol.*
d) Check the box *connect to a command-line hosts:* select the option below *use terminal window.*
e) Select *OK*, this will return you to the previous menu.
f) Proceed to login as normal.
g) Once you have connected, a terminal window will appear prompting you for your login. ❑